



Answers to Senate Questions Regarding Maricopa County Election Network:

Arizona 2020 Presidential Election

Former Congressman John Shadegg, Special Master

March 23, 2022

Summary of Process & Answers

Pursuant to an Agreement between the Arizona State Senate and Maricopa County (“the parties”), a special master was designated by the parties to review and answer certain questions posed by the State Senate relating to the conduct of the 2020 general election and the security of the County’s election network by examining the routers and Splunk logs which were part of that network. The special master was authorized to hire up to three independent computer security experts to answer the Senate’s questions. This document sets forth and explains the answers to those questions.

The Task Assigned

Background:

As a part of its audit of the Maricopa County 2020 general election, the Arizona State Senate sought to examine the equipment used by the County to tabulate the votes cast in the election including the County’s routers and certain log files (Splunk logs). The County objected to such an examination on the basis that the County’s routers and log files contain unrelated information that could lead to the disclosure of confidential, private, and protected data, access to which is strictly limited by law. The County asserted that it could not allow the Senate or any of its contractors to access the computers and associated equipment.

The County turned over its election management equipment including its tabulating machines, and other equipment but not its routers and Splunk logs. Following an extended legal dispute in which the Court upheld the Senate’s subpoenas an out-of-court Settlement Agreement was reached whereby the parties jointly agreed to the appointment of a special masterⁱ to examine the routers and Splunk logs in the County’s election network and answer questions submitted by the Senate. A copy of that Settlement Agreement is attached as Exhibit A.

Limited Scope of the Inquiry and Answers:

The Agreement specifically limits the inquiry to “the County’s routers and Splunk logs as they relate to the November 3, general election” with the relevant time period for the inquiry to be “from October 7, 2020, through November 20, 2020.”

The questions presented by the Senate focused on (1) “whether there was any evidence that the routers or managed switches in the election network connected to the public Internet,” (2) “[h]ow... the routers and managed switches in the election network were secured against unauthorized or third-party access,” and (3) “whether the routers or Splunk logs contain any evidence of data deletion, data purging, data overwriting or other destruction of evidence or obstruction of the audit.”

The Senate’s questions further instructed the special master with his team of experts to consider and explain whether any of a list of 57 separate “outputs” and specifically listed factors “supports or undermines” the answers to the Senate’s questions. A copy of the questions presented by the State Senate is attached as Exhibit B.

These are the only questions presented by the State Senate and the only questions the special master and his team of experts were authorized and/or directed to consider, examine, and answer. The special master and the expert panel who examined the County's election network as a part of this assignment did not consider, examine, or analyze any other questions, issues, allegations or assertions of any kind, [including physical handling of ballots, polling locations, other electronic records if any, mechanical, legal, or procedural questions of any nature whatsoever] which could, or purportedly could have, impacted the results of the 2020 general election in Maricopa County.

Special Master and Experts

The Agreement by the parties designates former Congressman John Shadegg, working with up to three technical experts, "to coordinate the process whereby answers will be provided to questions the Senate has concerning the County's routers and Splunk logs as they relate to the November 3, 2020, general election." Former Congressman Shadegg had extensive knowledge of Arizona's election process having advised the Arizona Secretary of State's office on election matters and represented it in election litigation and having advised the Maricopa County Recorder's office on election and redistricting matters prior to serving in Congress.

Technical Expert Selection Process

The special master was authorized to hire up to three experts with expertise in digital forensics and cyber threat analysis to assist in answering the questions presented by the State Senate. The process established for selecting these experts

was to allow each party (i.e., the Arizona State Senate and Maricopa County) to identify and nominate an expert of their choice. These two individuals were then vetted for potential conflicts of interest.

Following the vetting process, the experts selected by the parties jointly selected a third independent expert. In the course of this process one or more potential experts withdrew or was disqualified. The final three experts chosen to advise the special master in answering the Senate's questions were:

- Brad Rhodes (Colorado) - Gannon University (Pennsylvania)
- Andrew Keck (Ohio) – Profile Discovery (Ohio)
- Jane Ginn (Arizona) – Cyber Threat Intelligence Network (Delaware)

Their resumes are attached as Exhibits C, D & E.

Arizona State Senate Questions

Following the selection of the panel of experts the Arizona State Senate submitted its questions, Attached as Exhibit D. It is important to note that the Senate's questions are limited as to:

1. The topic - the 2020 general election;
2. The time-period - October 7th, 2022, through November 20th, 2022; and
3. The equipment and data - the Maricopa County routersⁱⁱ and managed switchesⁱⁱⁱ and Splunk logs^{iv}.

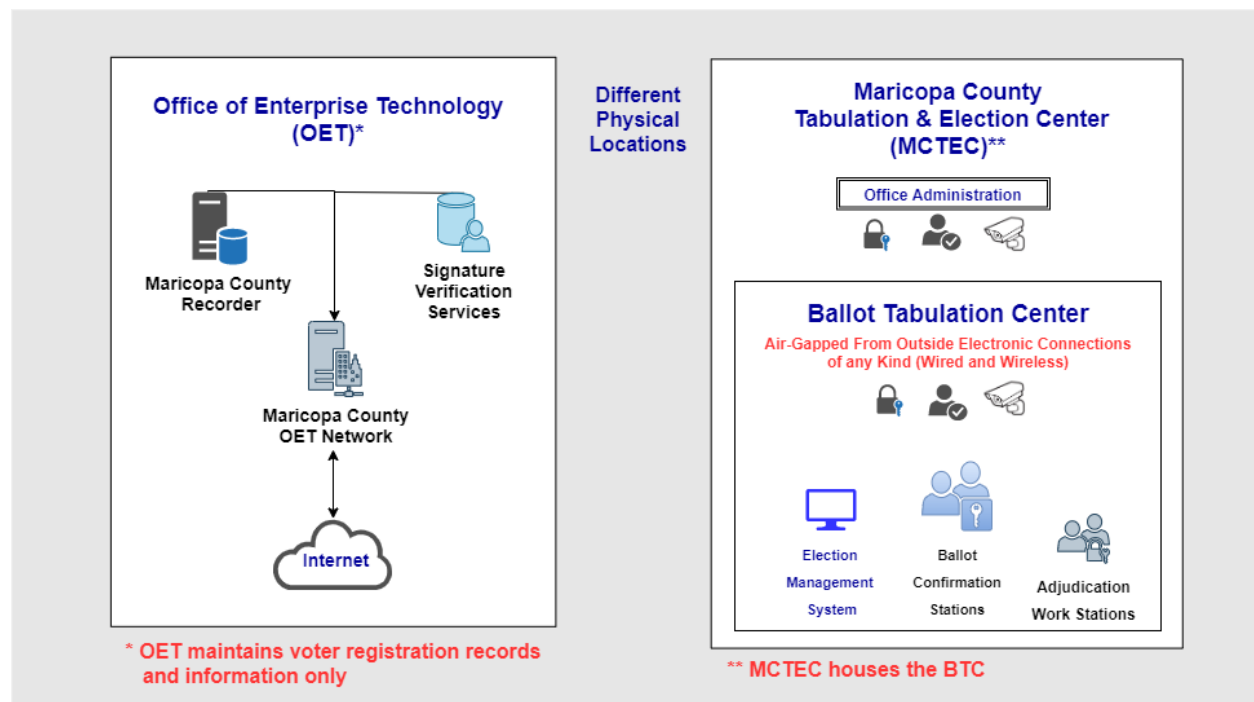
It is also important to note that the questions refer specifically to the routers and Splunk logs in “the election network”. A router is an electronic device which

organizes and directs communication between computer networks. It takes data packets from devices and directs them to where they need to go. They allow computers to access the Internet or request files from a server. A Splunk log is a centralized record or "log" that serves as an analysis tool for machine generated data from multiple sources.

The County "Election Network"

The term the "election network" is not defined and the questions appear to have been written based on the assumption that Maricopa County utilizes a single "election network". Upon inspecting the County's facilities and equipment the special master and expert panel found that there are actually two separate facilities and two completely separate computer systems utilized by the County to conduct elections as illustrated in Figure 1.

Figure 1: Diagram of Two Different Systems Which Comprise Election Network



This utilization of separate systems, which are physically separated and are not electronically connected, either by wire or wirelessly, is a critical factor in answering the Senate's questions.

An understanding of the purpose and function of these separate systems is central to the answers to the Senate's questions, provided below.

The Office of Enterprise Technology (OET)

The Office of Enterprise Technology (OET) provides the computer infrastructure for the County including all County departments. With respect to elections, the OET only stores and maintains voter registration records including original registration forms with the voter's signature (which is used to confirm the identity of voters who vote by mail), and other registration information. OET plays no role in the vote tabulation process. It is located in a facility separated from the Ballot Tabulation Center (BTC) and not connected to the BTC electronically, either by wire or wirelessly.

Maricopa County Tabulation and Election Center (MCTEC) and the Ballot Tabulation Center (BTC)

As referenced above, the second system/network utilized in the election process is the Ballot Tabulation Center (BTC) which is situated inside the Maricopa County Tabulation and Election Center (MCTEC). The BTC is inside but physically separated and not electronically connected, either by wire, or wirelessly, to OET or to any computer or computer network outside the BTC.

Physical access is restricted 24-hours a day / 7 days a week and is controlled by locked doors with card key access only and by continuous video monitoring.

To answer the Arizona State Senate’s questions the panel and the special master visited both of the physical facilities and examined the equipment and systems data as specified. The expert panel and special master visited the BTC, located inside MCTEC, and OET located in a different physical location.

Vote Tabulating Equipment

The vote tabulating equipment used to for the 2020 election has been replaced as part of the State Senate audit and is sequestered at the request of the Attorney General. The special master and the expert panel did inspect the equipment present for our visit and confirmed with the County that the vote tabulating machines at the BTC during the 2020 General Election and the new machines currently within the BTC were not, are not now, and are not ever connected by wire or wirelessly to any routers, computers, or electronic equipment outside the BTC. There are no routers and no managed or unmanaged switches in the BTC. And there are no electronic connections (wired or wireless) into or out of the BTC. There are no Splunk logs for the vote tabulating machines in accordance with privacy requirements of the Arizona Constitution. There are no Splunk logs in the BTC.

Text of Section 1:

Method of Voting; Secrecy

“ All elections by the people shall be by ballot, or by such other method as may be prescribed by law; Provided, that secrecy in voting shall be preserved. ”

Source: Article VII of the Arizona Constitution

Answers to Senate Questions 1 through 3

Because the County uses two separate systems in what could be considered its “election network” the special master and expert panel’s answers are set forth separately, one for the BTC and one for the OET.

Question #1: *Is there any evidence that the routers or managed switches in the election network, or election devices (e.g., tabulators, servers, signature-matching terminals, etc.), have connected to the public Internet?*

Answer for BTC:

No. The special master and expert panel found no evidence that the routers, managed switches, or election devices connected to the public Internet. There are no routers or managed switches or Splunk logs in the BTC.

Answer for OET:

The routers and/or managed switches in the OET do connect to the public Internet. However, the only election related information in the OET is registration information and records. The OET plays no role in the ballot tabulation process, and it is never connected, by wire or wirelessly, to the BTC or to any equipment in the BTC, which is air-gapped from the OET and all outside equipment or systems. No ballot tabulation information is ever received by, sent to or stored in the OET.

Question #2: *How, if at all, were the routers and managed switches in the election network secured against unauthorized or third-party access? Is there any evidence of such access?*

Answer for BTC:

The special master and expert panel found that there were no routers (or managed switches or Splunk logs) in the BTC. The BTC and the equipment in it are secured by card key access controls and continuous video surveillance preventing unauthorized or third-party access.

Answer for OET:

The OET is secured from outside physical access by unauthorized personnel by County personnel. The routers and managed switches in it do connect to the public Internet. However, the only election related information in the OET is registration information and records. The OET plays no role in the ballot tabulation process, and it is never connected, by wire or wirelessly, to the BTC or to any equipment in the BTC, which is air-gapped from the OET and all outside equipment or systems. No ballot tabulation information is ever received by, sent to or stored in the OET.

Electronic access to the equipment in the OET is continuously monitored by County personnel. Access to registration information has been detected as a result of this monitoring, it was blocked, and the name of the person involved, and the details of the incident were turned over to the Arizona Attorney General for prosecution. Details of this incident appear at item II on page 17 in the Detailed Explanation of Expert Panel Findings.^v

Question #3: *Do the routers or Splunk logs contain any evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit?*

Answer for BTC:

The special master and expert panel found no evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit.

Answer for OET:

The special master and expert panel found no evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit.

Detailed Explanation of Expert Panel Findings

Questions from the Senate	Expert Panel Responses	
	Ballot Tabulation Center [BTC] (Air-Gapped from Rest of Maricopa County Network)	OET Notes (Voter Registration DB & Recorder's Office)
1. Is there any evidence that the routers or managed switches in the election network, or election devices (e.g., tabulators, servers, signature-matching terminals, etc.), have connected to the public Internet?	<p>The special master and expert panel found NO evidence that the routers, managed switches, or elections devices connected to the public Internet.</p> <p>The special master and expert panel were allowed access to the Maricopa County Tabulation and Elections Center (MCTEC) and the Ballot Tabulation Center (BTC). There are no routers or managed switches or Splunk logs in the BTC. The special master and expert panel determined that the airgap</p>	<p>The routers and/or managed switches in the OET do connect to the public Internet. However, the only election related information in the OET is registration information and records. The OET plays no role in the ballot tabulation process, and it is never connected, by wire or wirelessly, to the BTC or to any equipment in the BTC, which is air-gapped from the OET and all outside equipment or systems. No ballot tabulation</p>

	<p>provides the necessary isolation from the public Internet, and in fact is in a self-contained environment. There are no wired or wireless connections in or out of the Ballot Tabulation Center. There are no routers, Splunk logs or Internet connections in the BTC. As such, the election network and election devices cannot connect to the public Internet. On-site walk-through of Elections Board Office. Oral briefing by Scott Jarret. ^{vi}</p>	<p>information is ever received by, sent to or stored in the OET.</p>
<p>2. How, if at all, were the routers and managed switches in the election network secured against unauthorized or third-party access? Is there any evidence of such access?</p>	<p>The special master and expert panel found that there are NO routers (or managed switches or Splunk logs) in the BTC within MCTEC. The BTC is secured by card key access controls and continuous video surveillance preventing unauthorized or third-party access.</p> <p>The special master and expert panel reviewed and confirmed that the MCTEC uses Critical Security Controls within the BTC, including physical access control to the servers, (unmanaged) switches, Ethernet port blockers, and 24/7 video surveillance. Our review was of the active center. There are no routers or Splunk logs in the BTC. There are no managed switches in the BTC. All elections systems in use are certified by the Election Assistance Commission (EAC). The BTC facility provides extensive physical security through card key access and 24-hour video surveillance to protect from unauthorized third-party access.</p>	<p>The OET is secured from outside physical access by unauthorized personnel by County personnel. The routers and managed switches in it do connect to the public Internet. However, the only election related information in the OET is registration information and records. The OET plays no role in the ballot tabulation process, and it is never connected, by wire or wirelessly, to the BTC or to any equipment in the BTC, which is air-gapped from the OET and all outside equipment or systems. No ballot tabulation information is ever received by, sent to, or stored in the OET.</p> <p>Electronic access to the equipment in the OET is continuously monitored by County personnel. Access to registration information has been detected as a result of this monitoring, it was blocked, and the name of the person involved, and the details of the incident were turned over to the Arizona Attorney General for prosecution. Details of this incident appear at item II on page 17 in the Detailed Explanation of Expert Panel Findings. ^{vii}</p>

3. Do the routers or Splunk logs contain any evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit?	<p>No. The special master and expert panel found no evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit.</p> <p>In the Ballot Tabulation Center, there are no routers or centralized logging (e.g., Splunk). As such, there is no evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit to review.</p>	<p>The special master and expert panel found no evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit.</p> <p>In reviewing the data from Maricopa County (outside of the air gapped BTC), there is no evidence of deletion, purging, overwriting, or destruction of logs or system data related to the audit.</p>
4. In preparing and in support of your answer to each of the foregoing questions, please consider and explain whether each of the following supports or undermines your previous answers and, further, provide copies of each of the following:	Pertaining to the BTC investigation, most these requests are not applicable. The applicable questions are addressed here:	Configuration details and Splunk logs were provided by Maricopa County to the special master and expert panel for the OET systems within the scope of this review. Maricopa County uses Splunk ES, (current Version 7.0 ~ which was the most up-to-date version during the timeframe). Policy is to maintain most up-to-date versions and to patch upon testing.
a. output from the show clock detail command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. Such data is only valuable if it is examined at the time in question. The special master and expert panel were not present during the 2020 elections and, therefore, cannot examine output from the show clock detail command.
b. output from the show version command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped.
c. output from the show running-config command	N/A - NO Routers or Splunk logs	Reviewed data available, as this is a dynamic command and results change over time pending regular maintenance.
d. output from the show startup-config command	N/A - NO Routers or Splunk logs	Reviewed data available, as this is a dynamic command and results change over time pending regular maintenance.
	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped.

e. output from the show reload command		
f. output from the show ip route command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
g. output from the show ip arp command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
h. output from the show users command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
i. output from the show logging command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
j. output from the show ip interface command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
k. output from the show interfaces command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
l. output from the show tcp brief all command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
m. output from the show ip sockets command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
n. output from the show ip nat translations verbose command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.

o. output from the show ip cache flow command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
p. output from the show ip cef command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
q. output from the show snmp user command	N/A - NO Routers or Splunk logs	Reviewed data available, normal operations - nothing applicable to this task.
r. output from the show snmp group command	N/A - NO Routers or Splunk logs	Reviewed data available, normal operations - nothing applicable to this task.
s. output from the show clock detail command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
t. output from the show audit command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
u. output from the show audit filestat command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
v. output from the show access-list command	N/A - NO Routers or Splunk logs	Reviewed data available, access control lists observed match county network diagram.
w. output from the show access-list [access-list- name] for each access list contained on each router	N/A - NO Routers or Splunk logs	Reviewed data available which included access-lists for specific connectivity. The access-lists assessed matched the county network diagram shown.
x. output from the show access-list applied command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped.
y. output from the show routing table command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results

		change over time pending regular maintenance.
z. output from the show ARP command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
aa. listing of all interfaces, the MAC address for each interface and the corresponding IP addresses for each MAC	N/A - NO Routers or Splunk logs	Reviewed data available which included MAC and IP addresses for the interfaces; normal operations observed.
bb. output from the show IP ARP command for each of the IP addresses associated with the router	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped. This is a dynamic command and results change over time pending regular maintenance.
cc. results of the write core command	N/A - NO Routers or Splunk logs	Specific data not available for the timeframe scoped.
dd. listing of all current and archived router configuration files (including the name, date of creation, date of modification, size of the file and hash valued of each configuration file)	N/A - NO Routers or Splunk logs	Reviewed archived router configuration files for the timeframe scoped. Current router configuration files are not relevant to the timeframe in question. Some included dates and users/systems accounts that made modifications. None were hashed.
ee. the routing table and all static routes	N/A - NO Routers or Splunk logs	Reviewed the available data, the majority of routes configured are dynamic and cannot be directly reviewed. Static routes available were assessed and determined to be mapped for critical inter-agency connections.
ff. a listing of all MAC addresses for all devices (tabulators, poll books, HiPro Scanners, ICC, Adjudication Workstations, EMS Workstations, and Election Management Server, etc.) utilized in the November 2020 general election	Data unavailable. Equipment used in the 2020 election is currently sequestered at the request of the Attorney General of Arizona.	N/A

gg. reports from the Router Audit Tool	N/A - NO Routers or Splunk logs	Router Audit Tool was not used because it is designed to assess current operational configurations (and potential vulnerabilities) which are now different from what they were in time frame scoped.
hh. Complete listing of the Splunk indexers including the MAC address and IP address for each indexer	N/A - NO Routers or Splunk logs	Listing of eleven Splunk indexers, MAC addresses, and IP addresses were provided and assessed. No concerns were noted.
ii. collective analysis, using Red Seal, of all routers contained in the Maricopa County network and routing reports to the Internet for each interface (including any routes that would allow connections from the 192.168.100.x, 192.168.10.x and 192.168.5.x subnets)	N/A - NO Routers or Splunk logs	Maricopa County does not use Red Seal (vulnerability scanner). Maricopa County uses vendor tools to run health checks - Annual Assessments for compliance. Reviewed routing information provided in available configuration files. County is unable to reconstruct memory details for time window given that traceroute information would only reside in memory.
jj. netflow data for the voting network and all other networks leading to the gateway router(s) that have Internet access containing the following data elements for each data transmission:	There is no netflow data for the "voting network" at the MCTEC. The voting network is air-gapped (in other words, not connected to Internet). The switches used to connect the voting network system are "un-managed" (plug 'n play) and no logs or netflow data are collected. As such this data does not exist.	N/A
• Date	N/A - NO Routers or Splunk logs	N/A
• Source MAC Address	N/A - NO Routers or Splunk logs	N/A
• Source IP Address	N/A - NO Routers or Splunk logs	N/A
• Source Port	N/A - NO Routers or Splunk logs	N/A
• Destination MAC Address	N/A - NO Routers or Splunk logs	N/A
• Destination IP Address	N/A - NO Routers or Splunk logs	N/A

• Destination Port	N/A - NO Routers or Splunk logs	N/A
• Type of protocol	N/A - NO Routers or Splunk logs	N/A
• Size of the packet	N/A - NO Routers or Splunk logs	N/A
kk. Splunk data containing the following data elements at a minimum:	This question is not applicable to these systems.	Splunk data in the form of configuration files, event, firewall, and router log records were given for the relevant systems in the scope. Splunk logs provided included the data specified.
• Date	N/A	Available data was reviewed as needed.
• Source MAC Address	N/A	Available data was reviewed as needed.
• Source IP Address	N/A	Available data was reviewed as needed.
• Source Port	N/A	Available data was reviewed as needed.
• Destination MAC Address	N/A	Available data was reviewed as needed.
• Destination IP Address	N/A	Available data was reviewed as needed.
• Destination Port	N/A	Available data was reviewed as needed.
• Type of protocol	N/A	Available data was reviewed as needed.
• Size of the packet	N/A	Available data was reviewed as needed.
• Any affiliated Splunk alert or notification data	N/A	Available data was reviewed as needed.
ll. Netflow and Splunk data related to any unauthorized access by Elliot Kerwin or his affiliates of the Maricopa County registration server and/or network	N/A	An unauthorized member of the public used a PowerShell script with sequential low egress parameters for harvesting information from the voter registration database. The individual was taking 'screenshots' of voter registration information. County staff remediated to restrict website access and referred case to State Attorney General. Arrest was made December 5th, 2020. Case No. 20-3262MB. ^{viii}

mm. all Splunk data related to the following windows logs on the EMS Server: EMS Workstations, Adjudication Workstations, ICC systems, HiPro Scanners, and the Poll Worker laptops	There is no Splunk system in the BTC. Therefore, there are no Splunk data available for the systems listed. The equipment used in the 2020 election is currently sequestered at the request of the Attorney General of Arizona. Laptops at polling places are never connected to the BTC and play no role in the ballot tabulation process.	N/A
--	---	-----

Conclusions

There is consensus among the panelists that our conclusions are based on a high level of confidence with respect to the information that we reviewed. Furthermore, in conclusion we would like to reiterate these key points:

1. There are two separate computer networks that comprise the Maricopa County election network. One exclusively stores and maintains registration records and information only (OET). The other tabulates election results only. This is the BTC. It is physically and electronically separated from the outside. The BTC is monitored 24 hours a day, 7 days a week, and is accessible only by authorized personnel with card key access. There is no electronic connection between the BTC and the MCTEC, either wired or through a wireless protocol.
2. There are no routers in the BTC.
3. No Splunk logs were available for review of the BTC network within the MCTEC because none were generated as described above.
4. The Voter Registration database (from OET) is never transmitted electronically to the BTC in accordance with the privacy provisions of the Arizona Constitution.

-
5. Vote tallies, as they are completed, are loaded on a newly opened USB (thumb drive, Flash drive), under the observation of politically appointed observers, and are then physically taken out of the BTC and loaded on a separate computer for distribution to the press and public
 6. The official canvass is also loaded on a newly opened USB (thumb drive, or Flash drive) and is hand carried to the Secretary of State's office along with chain of custody control documentation.

The USBs taken out of the BTC are loaded on separate computers and the information is disseminated to the Secretary of State's office and the County website. The USBs are returned to the BTC and ultimately saved for historical purposes.

References:

ⁱ The special master was selected by the parties, not the Court, and is designated in the Agreement, included in this report as Exhibit A.

ⁱⁱ A router is responsible for organizing communication between computer networks. A router takes data packets from devices and directs them to the right place. Routers often use IP addresses to know where to look for information. Routers allow your computers to access the Internet or request files from a server.

ⁱⁱⁱ The Arizona State Senate also asked the Panel to determine if there were “managed switches” in the “election network”. A managed switch enables better control of networks and the data frames moving through them; however, a managed switch requires a network engineer to configure them. Unmanaged switches, on the other hand, enable connected devices to communicate with one another in their most basic form. One of the questions posed by the Senate referenced managed switches.

^{iv} Splunk is centralized logs analysis tool for machine generated data, unstructured/structured and complex multi-line data which provides the following features such as Easy Search/Navigate, Real-Time Visibility, Historical Analytics, Reports, Alerts, Dashboards and Visualization.

^v Voter Registration Data is maintained by both Maricopa County and IBM through the ServiceArizona.com Website. County maintains an SQL database internally at <https://recorder.maricopa.gov/beballotready/> . State sync's with ServiceArizona which is maintained by IBM's security services.

^{vi} January 7, 2022 - Correcting the Record You Tube Video (<https://www.youtube.com/watch?v=VjNIGcmi2jY>)
Correcting the Record PDF Download (available to download at:

<https://www.documentcloud.org/documents/21174009-correcting-the-record-january-2022-report?responsive=1&title=1>). Extensive 'Correcting the Record' Report with Appendices published by Maricopa County.

^{vii} Voter Registration Data is maintained by both Maricopa County and IBM through the ServiceArizona.com Website. County maintains an SQL database internally at <https://recorder.maricopa.gov/beballotready/> . State sync's with ServiceArizona which is maintained by IBM's security services.

^{viii} <https://www.azcentral.com/story/news/local/phoenix/2020/12/05/law-enforcement-investigates-voter-data-theft-maricopa-county/3834588001/>
<https://www.forbes.com/sites/thomasbrewster/2020/12/04/exclusive-the-fbi-is-investigating-voter-data-theft-in-this-key-2020-election-battleground/?sh=1c74988734a4>

Exhibit A

AGREEMENT

This Agreement is entered into by and between Maricopa County through its Board of Supervisors ("County") and the Arizona State Senate ("Senate") known as ("the Parties") and is effective on the date signed by the last Party to date and sign the Agreement.

Whereas the Senate issued subpoenas signed by its President and the Chair of its Judiciary Committee and dated January 12, 2021 and July 26, 2021, directed to Maricopa County Board of Supervisors; and

Whereas the County has fully complied with the subpoenas, except it has not provided the subpoenaed routers and splunk logs, citing security concerns, and also has not provided certain subpoenaed passwords and security tokens that the County does not possess; and

Whereas the Attorney General issued a Report finding the County's noncompliance a violation of state law; and

Whereas the County disputes the Attorney General's finding; and

Whereas the County has notified the Senate and the state of Arizona that the County has a claim for money damages against the Senate and the State related to costs it incurred replacing equipment that was subject to the Senate's subpoenas; and

Whereas the Parties wish to amicably settle their differences;

IT IS HEREBY AGREED:

1. A Special Master has been selected by the Parties to coordinate the process whereby answers will be provided to questions the Senate has concerning the County's routers and splunk logs as they relate to the November 3, 2020 general election. The Special Master is former congressman John Shadegg. Congressman Shadegg will hire one to three computer technology experts to assist him in responding to the Senate's questions,

2. The Special Master shall have the sole authority to hire his expert team. Each team member will sign a confidentiality and non-disclosure agreement stating that no information the team member acquired during their employment will be disclosed, revealed, released, published or otherwise disseminated to any person or entity, other than the Special Master.

3. The scope of the Senate's questions shall be limited to matters concerning the County's routers and splunk logs in relation to the November 3, 2020 general election. The relevant time period shall be from October 7, 2020 through November 20, 2020. The Special Master will disclose the questions posed by the Senate's counsel to the County's counsel and allow the parties an opportunity to brief any purported grounds for withholding some or all of an answer to the question. The Special Master will provide the answers in their entirety to the Senate and the County, provided that the Special Master will not communicate answers only if and to the extent they

disclose (i) attorney-client privileged communications of the County, (ii) nonpublic information relating to the Maricopa County Sheriff's Office or other law enforcement agencies, (iii) nonpublic information relating to the Maricopa County Superior Courts and/or information otherwise prohibited from disclosure by the Arizona Rules of the Supreme Court or (iv) the personal identifying information of any individual. For purposes of this section, the term "personal identifying information" shall include an individual's date of birth, Social Security number or protected health information, but shall not include an individual's name or usernames or passwords associated with a County computer system. The decision of the Special Master on such matters will be final. In the event that information sought by the Senate is not available, the Senate and the County shall be so informed. The answers to the Senate's questions will be shared only with the Senate and the County through their respective counsel. The Special Master will not be required to prepare a report.

4. The Special Master and his team will work with appropriate security protocols in place to prevent the disclosure of any information they acquire. The Special Master and his team will have no connectivity to the internet while conducting searches of the County computer equipment. The Special Master and his team will not copy (to any device or in any form) any of the information they review or observe during the course of their work.

5. Any subpoena or court ordered production of information made of the Special Master shall be immediately conveyed to counsel for both the Senate and the County so either party can seek relief from production if needed.

6. The County agrees to forever waive and release its claim referenced in its Notices of Claim served on Senate President Fann and dated August 18, 2021 and August 23, 2021, related to the County's replacement of its election equipment that had been delivered to the Senate pursuant to the January 12, 2021 subpoena, and any other claim or cause of action arising out of the Covenant of Indemnification by and between the Arizona Senate and Maricopa County dated April 20, 2021.

7. The County agrees to produce any digital images of ballot envelopes, which were commanded to be produced by the July 26, 2021 subpoena and that have not yet been produced at the time of the signing of this agreement, if any, no later than September 22, 2021.

8. The County agrees to pay all costs for the employment of the Special Master and his staff and not seek indemnification or damages from the Senate.

9. The Senate agrees that upon execution of this Agreement, President Fann will send on the same day she executes this Agreement both an email and a USPS letter to the Arizona Attorney General stating that the County has fully complied with the Senate's outstanding subpoenas and further action on his part is not warranted.

10. This Agreement constitutes the entirety of the agreements of the Parties and may not be amended or otherwise altered or changed except in writing and signed by the Parties.

Exhibit B

Questions from the Arizona State Senate to Special Master John Shadegg

1. Is there any evidence that the routers or managed switches in the election network, or election devices (*e.g.*, tabulators, servers, signature-matching terminals, etc.), have connected to the public internet?
2. How, if at all, were the routers and managed switches in the election network secured against unauthorized or third party access? Is there any evidence of such access?
3. Do the routers or splunk logs contain any evidence of data deletion, data purging, data overwriting, or other destruction of evidence or obstruction of the audit?
4. In preparing and in support of your answer to each of the foregoing questions, please consider and explain whether each of the following supports or undermines your previous answers and, further, provide copies of each of the following:
 - a. output from the show clock detail command.
 - b. output from the show version command.
 - c. output from the show running-config command.
 - d. output from the show startup-config command.
 - e. output from the show reload command.
 - f. output from the show ip route command.
 - g. output from the show ip arp command.
 - h. output from the show users command.
 - i. output from the show logging command.
 - j. output from the show ip interface command.
 - k. output from the show interfaces command.
 - l. output from the show tcp brief all command.
 - m. output from the show ip sockets command.
 - n. output from the show ip nat translations verbosecommand.
 - o. output from the show ip cache flow command.
 - p. output from the show ip cef command.
 - q. output from the show snmp user command.
 - r. output from the show snmp group command.
 - s. output from the show clock detail command.
 - t. output from the show audit command.
 - u. output from the show audit filestat command.
 - v. output from the show access-list command
 - w. output from the show access-list [access-list-name] for each access list contained on each router.
 - x. output from the show access-list appliedcommand.
 - y. output from the show routing table command
 - z. output from the show ARP command.
 - aa. listing of all interfaces, the MAC address for each interface and the corresponding IP addresses for each MAC.
 - bb. output from the show IP Arp command for eachof the IP addresses associated with the router.
 - cc. results of the write core command.
 - dd. listing of all current and archived router configuration files (including the name, date of creation, date of modification, size of the file andhash valued of each configuration file).

- ee. the routing table and all static routes.
- ff. a listing of all MAC addresses for all devices (tabulators, poll books, HiPro Scanners, ICC, Adjudication Workstations, EMS Workstations, and Election ManagementServer, etc) utilized in the November 2020 general election.
- gg. reports from the Router Audit Tool.
- hh. Complete listing of the Splunk indexers including the MAC address and IP address for each indexer.
- ii. collective analysis, using Red Seal, of all routers contained in the Maricopa County network and routing reports to the internet for each interface (including any routes that would allow connections from the 192.168.100.x, 192.168.10.x and 192.168.5.x subnets).
- jj. netflow data for the voting network and all other networks leading to the gateway router(s) that have internet access containing the following data elements for each data transmission:
 - Date
 - Source MAC Address
 - Source IP Address
 - Source Port
 - Destination MAC Address
 - Destination IP Address
 - Destination Port
 - Type of protocol
 - Size of the packet.
- kk. Splunk data containing the following data elements at a minimum:
 - Date
 - Source MAC Address
 - Source IP Address
 - Source Port
 - Destination MAC Address
 - Destination IP Address
 - Destination Port
 - Type of protocol
 - Size of the packet.
 - Any affiliated Splunk alert or notification data
- ll. netflow and splunk data related to any unauthorized access by Elliot Kerwin or his affiliates of the Maricopa County registration server and/or network.
- mm. all splunk data related to the following windows logs on the EMS Server: EMS Workstations, Adjudication Workstations, ICC systems, HiPro Scanners, and thePoll Worker laptops.

For each of the foregoing questions, please limit your answers to the time period beginning on October 7, 2020 and ending on November 20, 2020.

Exhibit C

Brad Rhodes

Aurora, Colorado, United States



[Linkedin.com/in/brad-rhodes-1951ba7](https://www.linkedin.com/in/brad-rhodes-1951ba7)

Summary

Cybersecurity Engineer specializing in: Defense, Vulnerability Assessments, Threat Intelligence, Hunting, Incident Response, Risk Management, & Exercise Design

Professional Certifications: CISSP-ISSEP, ISACA (CISM, CDPSE), PMP, GIAC (GLEG, GCED, GMON, & GCIH), EC-Council (C|EH, CNDA, CTIA, & E|CIH), CompTIA (CASP+, CySA+, Security+, PenTest+, Linux+, & Cloud+), RHCSA, CCII, Safe Agilist

24+ years of professional experience with multiple specialties: defensive cyber operations (US Army Cyber Officer), incident response and handling, vulnerability assessments kinetic-cyber simulation implementation, blue vs red team cyber exercises (planning and execution), cyber risk management, information operations (incident communications and messaging (qualified US Army IO Officer)), geospatial information systems/intelligence (certified in Collection Operations), space operations (qualified US Army Space Operations Officer), satellite communications (wideband, protected, narrowband, and commercial systems), systems engineering disciplines, export control regulations and implementation, and policy and procedures development.

Goals: Lifelong learning and growth leading to continued success in both my civilian and military (Army Reserve) careers balancing my priorities of faith, family, and service.

Experience



COL, Cyber Warfare (Part Time)

US Army

Aug 2021 - Present (6 months +)

COL, Cyber Warfare Officer

Information Operations & Space Operations Functional Areas

Current: G6/Chief Information Officer, 76th Operational Response Command (US Army Reserve)

Major responsibilities include:

- Delivering mission critical communications for 7000+ personnel assigned to the 76th
- Ensuring cybersecurity compliance for all unit systems
- Managing technology transitions including A365 and future BYOD support
- Preparing for Defense Support of Civil Authorities (DSCA) response requirements directed by US Army North



Affiliate Professor (Part Time)

Regis University

Jan 2018 - Present (4 years 1 month +)

- Instructor for Regis University's Anderson College of Business & Computing (ACBC) focused on Ethical Hacking, Malware Analysis, Risk Management, and hands on capstone courses in Threat Intelligence and Incident Response.

- Concept development support for Cyber Exercises, Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC), and academic studies.



Adjunct Professor (Part Time)

Gannon University

Jan 2021 - Present (1 year 1 month +)

Adjunct Professor teaching Cybersecurity Leadership concepts for students looking to transition into the industry.



Instructor (Part Time)

ACI Learning

Apr 2021 - Present (10 months +)

Instructor for courses including:

- Certified Ethical Hacker (CEH)
- Security+



Head of Cybersecurity

zvelo, Inc.

Mar 2020 - Jan 2022 (1 year 11 months)

- Lead development of zvelo Cyber Threat Intelligence (CTI) malicious offerings integrating the Cyber Kill Chain and MITRE ATT&CK framework
- Developed first-ever Business Continuity Plan (BCP) for zvelo with vulnerability assessments and risk-based prioritization of fixes including cloud (Amazon Web Services)
- Customer support research into malicious and phishing domains (to confirm or deny)
- Primary contributor to zveloCTI Malicious Trends Report 2020 and 2021 (current report here: <https://zvelo.com/resources/threat-intelligence-reports/zvelocti-malicious-trends-report-2021/>)
- Framed the Tactic Technique & Procedure (TTP) of Living Off The Land at Scale (LOTLS) to describe threat actor use of free/low cost capabilities to host malware and other malicious content (<https://zvelo.com/living-off-the-land-at-scale/>)
- 2021 external presentations (O = Online, I = In-Person, R=Recorded): Rocky Mountain Information Security Conference (O), Peak Cyber Symposium (I), Space Education & Strategic Applications (O), Hacker Halted (O), VetSecCon (O), US Space Force Space Systems Command Cyber Expo (R), AvengerCon VI (O), and other panels as a Subject Matter Expert
- 2020 external presentations on (all online): Malicious COVID-19 research (<https://zvelo.com/zvelo-coronavirus-proactive-research/>), Cyber and Big Data, Cyber Basics, Transitioning Veterans, and the Intersection of Influence Operations and Malicious Infrastructure



LTC, Cyber Warfare (Part Time)

Army National Guard

May 2000 - Jul 2021 (21 years 3 months)

LTC, Cyber Warfare Officer

Information Operations & Space Operations Functional Areas

Last Assignment: Exercise OIC, Cyber Shield

Recent Accomplishments:

- Leading Cyber Shield '21 for 1000+ participants in Staff, Blue/Maneuver Teams, White/Assessments, Red/OPFOR, and Information Operations to execute real-time defensive cyber operations.
- Returned from deployment in support of Task Force Echo 3 (February 2020).
- Led Cyber Protection Team 174 to Full Operational Capability (February 2020).
- Cyber Shield 2018 Deputy Exercise Officer-in-Charge for 800+ personnel managing technical range operations and exercise event synchronization.
- Sr. Threat Hunter supporting the Colorado Department of Transportation ransomware incident response (Mar 2018).
- At Cyber Shield (Apr-May 2017), presented classes on Cyber-Intel for Leaders, Cyber-Tools for Leaders, and Cyber for Judge Advocate Generals.
- For the Feb 2017 "Dam Cyber Exercise" at Regis University built and coded a simulator using IoT (Raspberry Pi, Arduino, a micropump, servo, and LED lights) to represent critical infrastructure in a demo of kinetic-cyber effects.

Past:

Commander, Cyber Protection Team (CPT) 174 (January 2017-March 2020)

- Task Force Echo 3 (Jan 2019-Feb 2020)

Deputy G6/Defensive Cyber Operations-Element (DCO-E) Chief & Cyber Planner (Jan 2014-Dec 2016)

S3/Fires & Effects Cell/Information Ops, HQs, 169th Fires Brigade (March 2012-Dec 2013)

Army Space Support Team (ARSST) Leader, 1158th Space Support Company (Mar 2010-Feb 2012)

- Operation Enduring Freedom (Afghanistan) (Nov 2010-Sep 2011)

Commander, 217th Space Support Company (Dec 2008-Feb 2010)

Executive Officer, 117th Space Battalion (June-Nov 2008)

ARSST Leader, 217th Space Support Company (Nov 2005-May 2008)

Commander, 143rd Signal Company (Heavy Tropo) (Nov 2001-Nov 2005)

- Operation Noble Eagle (Mar-May 2002)

- Operation Iraqi Freedom (Dec 2003-May 2005)

Operations Officer, 140th Signal Company (Cmd & Ops) (May 2000-Oct 2001)



Instructor (Part Time)

Cybrary

Jul 2020 - Dec 2020 (6 months)

Creator of Cybrary's CISSP Information Systems Security Engineering Professional (ISSEP) concentration course. Launched 12/23/2020!



LTC, CY: Mission Management Team Chief

US Army

Jan 2019 - Feb 2020 (1 year 2 months)

- Mission Management Team Chief for Task Force Echo (TFE) leading upwards of 60+ personnel (organic, Joint (Air Force, Navy, Marines), Army Civilians, and contractors) supporting multiple teams across the Cyber National Mission Force in delivering more than 10,000 hours of full spectrum cyberspace operations. Managed Joint Mission Operations Center (JMOC) processes from Future Operations planning to daily Current Operations resulting in the execution of several thousand cyberspace missions. Provided the vision for TFE Knowledge Management leading to the complete documentation of all mission Standard Operating Procedures, Qualification Standards, and Playbooks (1000+ pages) for the first time ever.
- Emcee, mentor, and workshop presenter for AvengerCon IV (October 2019) (500+ attendees).

- While deployed for TFE, led CPT174 (39+ personnel) in achieving Initial Operating Capability (IOC) and Full Operating Capability (FOC) two and three years ahead of schedule. Coordinated for external support and built the 120+ virtual machine range utilized for the unit FOC Validation Exercise.
- Presented Incident Response “Lessons Learned” at FEMA National Level Exercise (NLE) Cyber Workshops in June, July, August, September, and October 2019 to over 400 attendees directly impacting preparedness for the 2020 Elections.
- Presented Army Cyber Talent Management at NIST’s National Initiative for Cybersecurity Education webinar in July 2019 to 70 attendees.



Senior Principal, Cyber Defense Manager

Defense Point Security, LLC (part of Accenture Federal Services)

Oct 2018 - Dec 2018 (3 months)

Cyber Threat Hunting, Cyber Threat Intelligence, and Cyber Defense Integration in support of internal and external customers. Leads engagements to secure customer environments, provides training & exercise support, and develops playbooks to grow community information sharing efforts. Hunt and incident response engagements including log analysis, malware analysis, and documentation.



Sr. Hunter/Security Manager

Accenture Federal Services

Aug 2017 - Sep 2018 (1 year 2 months)

Leads Cyber Threat Hunting teams in operational engagements with government and other organizations. Conducts Open Source Threat Intelligence research, aggregation, and analysis in support of external assessments. Provides both platform specific and tool-agnostic training classes as required. Develops training materials and documentation to support customer needs including: Endgame, ELK (Elasticsearch Logstash Kibana) stack(s), Graylog, and Security Onion. Scripting and automation with Python and Powershell.



Requirements & Integration Lead

National Geospatial-Intelligence Agency

Dec 2011 - Aug 2017 (5 years 9 months)

Requirements & Integration Team Leader developing "Big Data" metrics analysis and visualization solutions using tools including Anaconda, Microsoft Power BI, Tableau, and ELK stack. Previously, GEOINT Pathfinder Cyber Analyst responsible for using open sources to assess the current state of internet infrastructure in locations globally to answer questions for key decision makers. Developed methodologies using open source software and technology to create visualizations for packet capture (PCAP) files with 18 million+ records. Developed custom python scripts to conduct web-scraping of public-facing IP addresses and node geolocations.



Senior Systems Engineer

Apogee Engineering, LLC

Oct 2006 - Jul 2010 (3 years 10 months)

Supported HQ AFSPC/A5MC. Primary author developing Strategic Instruction (SI) 714-09: Protected SATCOM Systems for the Protected Consolidated SATCOM Systems Expert (C-SSE) role accepted HQ AFSPC. Develop the AFSPC MILSATCOM Responsibilities Plan (AMRP) and support POM inputs for ensuring command responsibilities are properly resourced. Supported multiple proposal

development projects. Additionally, served as the company Export Control Officer (ECO) for Apogee developing SOPs, training, and managing interactions with the Departments of State and Commerce.



Associate

Booz Allen Hamilton

Jan 2002 - Oct 2006 (4 years 10 months)

Supported HQ AFSPC/A6MZ and the AEHF International Partners (developed the AEHF IP CONSUP and CNIP). Supported SMC/OSL at the CISF on Peterson AFB implementing test and evaluation events across the AFCPT, SMART-T and SCAMP Milstar terminals. Supported ASD/NII in managing and streamlining overarching GIG policy documents.



Systems Engineer

Femme Comp Inc

May 2000 - Jan 2002 (1 year 9 months)

Supported HQ Army Space Command in the EHF Network Operational Manager (NOM). Developed the Joint EHF SAR/SAA/AAR. Trained in SMART-T and SCAMP terminal operations and MCPT-i communications planning. Provided SCAMP training to Special Operations Forces users at Fort Carson, CO. Led the first Army EHF Operations Working Group (AEOWG) at Fort Hood, TX.



1LT, Signal Corps

US Army

May 1997 - Apr 2000 (3 years)

Active Duty US Army stationed at Fort Gordon, GA.

Platoon Leader, 235th Signal Company (TACSAT)/67th Signal Battalion (Mar 1999-Apr 2000)

Asst S-3, Network Planning, 93rd Signal Brigade (Jun 1998-Mar 1999)

Asst S-3, Automations, 63rd Signal Battalion (Sep 1997-Jun 1998)

Student, SOBC Class 97-501 (May-Sep 1997)

Education



Swinburne University of Technology

Master of Science - MS, Astronomy

2001 - 2008



U.S. Army Command and General Staff College

2008 - 2009



Embry-Riddle Aeronautical University

BS, Aerospace Studies (Computer Science/Apps and Aviation Safety)

1993 - 1997

Licenses & Certifications



Certified Information Systems Security Professional (CISSP) - (ISC)²

Issued Jan 2018 - Expires Dec 2023

498915



GIAC Law of Data Security & Investigations - GLEG - GIAC Certifications

Issued Aug 2016 - Expires Aug 2023

727



Certified Ethical Hacker (C|EH) - EC-Council

Issued Feb 2017 - Expires Feb 2023



Secure Agile Framework (SAFe) Agilist - Scaled Agile, Inc.

Issued Apr 2015 - Expires Dec 2022



Certified Network Defense Architect - EC-Council

Issued Feb 2017 - Expires Feb 2023

ECC57077566822



GIAC Certified Enterprise Defender

Issued Oct 2018 - Expires Oct 2022

3288



Certified Information Security Manager - ISACA

Issued Dec 2018 - Expires Jan 2022

1843540



CompTIA Security+ ce Certification - CompTIA

Issued Aug 2017 - Expires Aug 2026

COMP001021578104



GIAC Continuous Monitoring Certification (GMON) - GIAC Certifications

Issued Dec 2018 - Expires Dec 2022

1911



CompTIA Linux+ ce Certification - CompTIA

Issued Oct 2018 - Expires Oct 2024

COMP001021578104



EC-Council Certified Incident Handler v1 - EC-Council

Issued Jan 2019 - Expires Jan 2022

ECC3694057218



Information Systems Security Engineering Professional (CISSP-ISSEP) - (ISC)²

Issued May 2014 - Expires Dec 2023

498915



GIAC Certified Incident Handler (GCIH) - GIAC Certifications

Issued Jul 2019 - Expires Jul 2023

35012



GIAC Advisory Board - GIAC Certifications

Issued Oct 2018 - Expires Jul 2023



Certified Cyber Intelligence Investigator (CCII) - McAfee Institute

Issued Jul 2019 - Expires Jul 2023

13330762



Red Hat Certified System Administrator (RHCSA) - Red Hat

Issued Sep 2019 - Expires Sep 2022

190-218-859



Project Management Professional (PMP) - Project Management Institute

Issued Oct 2019 - Expires Oct 2022

5963615



CompTIA Cybersecurity Analyst (CySA+) - CompTIA

Issued Nov 2019 - Expires Nov 2025

COMP001021578104



CompTIA Security Analytics Professional - CompTIA

Issued Nov 2019 - Expires Nov 2025

COMP001021578104



Certified Data Privacy Solutions Engineer - ISACA

Issued Apr 2021 - Expires Jan 2025

2117885



CompTIA Secure Cloud Professional - CompTIA

Issued Oct 2020 - Expires Oct 2023

COMP001021578104



CompTIA Cloud+ ce Certification - CompTIA

Issued Oct 2020 - Expires Oct 2023

COMP001021578104




CompTIA Advanced Security Practitioner ce Certification - CompTIA

Issued May 2021 - Expires May 2024


COMP001021578104


 **CompTIA Security Analytics Expert – CSAE Stackable Certification - CompTIA**
Issued May 2021 - Expires May 2024
COMP001021578104

 **CompTIA PenTest+ ce Certification - CompTIA**
Issued Jun 2021 - Expires Jun 2024
COMP001021578104

 **CompTIA Network Vulnerability Assessment Professional – CNVP Stackable Certification - CompTIA**
Issued Jun 2021 - Expires Jun 2024
COMP001021578104

 **CompTIA Network Security Professional – CNSP Stackable Certification - CompTIA**
Issued Jun 2021 - Expires Jun 2024
COMP001021578104

 **CompTIA Infrastructure Security Expert – CSIE Stackable Certification - CompTIA**
Issued Jun 2021 - Expires May 2024
COMP001021578104

 **Certified Threat Intelligence Analyst - EC-Council**
Issued Nov 2021 - Expires Nov 2024
ECC0927815634



Space Education & Strategic Applications 2021 Conference Presenter - American Public University System

Skills

Proposal Writing • Security Clearance • Command • Integration • Satellite Communications • DoD • Military • Training • Army • National Security

Andrew Keck – Expert Witness & Cyber Security Consultant

Exhibit D

Present Position

Chief Technology Officer -Owner 2006-Present

Profile Imaging of Columbus, LLC., d.b.a. ProFile Discovery
Columbus, Ohio

Previous Positions

General Manager 2003-2006

XACT Data Discovery, LLC
Columbus, Ohio

US ARMY NG/Reserves 1993-2005

375th MP Battalion
1486th Transportation
Ohio

Litigation Courtroom Technology Consultant 2000-2006

AYCS Graphics
Columbus, Ohio

Litigation Consultant 1998-2000

Visual Evidence
Cleveland, Ohio

Experience

Information Security, Compliance & Discovery

Andrew Keck works with law firms, government agencies, and fortune 1000 corporations during an investigation or court proceeding involving digital evidence requiring forensic and electronic discovery processes. Services range from advanced cyber security, computer and digital evidence identification, collection, preservation, processing, and presenting as evidence in the courtroom. As the CTO of Profile Discovery, a privately-owned entity in the State of Ohio, responsibilities include the following:

Introduce Electronic Discovery practices for the Columbus and Cleveland Profile Imaging offices, which later became Profile Discovery. Primary enterprise architect for IT hardware and industry specific software implementations to support various production requests from clients.

Supervise and provide leadership for IT and incident response teams responsible for the coordination of eDiscovery collections, including forensics, processing, SQL Database and evidence productions.

Andrew Keck – Expert Witness & Cyber Security Consultant

Supervise and conduct network forensics and examinations in cases involving Linux, Mac, PC, cloud-based, and mobile devices.

Provide leadership role while guiding IT teams responsible for the development and implementation of Profile Discovery forensic lab, Online hosting and data processing systems. These implementations include:

Deployment of VMware for penetration testing and cyber labs to ensure data regulations, and policy requirements are met across multiple on premise, data center, and Cloud based data management solutions.

Thought leader in implementing Microsoft SQL based IPRO eCapture Suite, on and off premise. SQL implementation for metadata extractions, text and native productions. IPRO Certified Sales expert.

Over ten years' experience working with AccessData Forensic Tool Kit and Microsoft SQL based Summation/Summation Pro enterprise electronic discovery, forensic and cybersecurity systems. Andrew introduced Summation Pro as an enterprise level forensic and Early case assessment tool to the company. AccessData Certified Examiner.

Over ten years' experience working in enterprise network systems with fortune 1000 corporations such as American Electric Power, Nationwide Insurance, and Ashland Oil providing network fingerprinting, data and digital evidence collections. Responsibility including database migrations, email collections in IBM Lotus notes, Microsoft Exchange, Microsoft 365, and Lexis Nexus Concordance for Litigation support.

Video productions and video editing solutions using Sony Vegas, Adobe Premiere and Final Cut PRO, Verdict Systems Sanction II and Trial Director for Demonstrative Evidence and trial presentation.

Solution research and development of mobile devices including iOS and Android devices using Katana based Lantern 4.0 to preserve digital evidence for Logical Mobile Forensics.

Train and supervise Cloud based discovery teams using industry standards and Total Discovery eCloud collections for cloud based forensic evidence collections.

Andrew Keck – Expert Witness & Cyber Security Consultant

IT Consultation on complex litigation cases regarding data collection, imaging and document management best practices.

Knowledge with Security Platforms including RSA, Accessdata, Alienvault, Carbon Black, and other cloud-based enterprise and endpoint solutions

ArcGis – Has worked with Geographical Information systems to plot data to maps, and vice versa.

Xact Data Discovery, LLC

Hired as an account manager in 2003. Helped consult and manage imaging projects and cases involving electronic evidence.

AYCS Graphics, LLC

Owned and operated AYCS to provide trial support through use of demonstrative evidence, accident reconstruction, video depositions and other courtroom specific technologies.

Visual Evidence, LLC

Hired as a Litigation Consultant to identify and consult with corporate legal departments in need of demonstrative evidence. Opened the Columbus location of Visual Evidence and established base network.

Education

Ashland University-1996

Bachelor of Arts. Double Major in Criminal Justice & Psychology
Ashland, Ohio.

Utica College-2016

Master of Science Cybersecurity – Specialization in Cyber Intelligence. Utica, New York.

Courses: Cybersecurity, Cyber Intelligence, Critical National Infrastructure & National Security, Principles of Cybercrime Investigation, Critical Communication and Incident Response, Advanced Topics in Cybersecurity, Residency, and Capstone I & II.

Andrew Keck – Expert Witness & Cyber Security Consultant

Certifications, Skills & Publications

AccessData Certified Examiner (ACE)
(Forensic Toolkit, Password Recovery Toolkit, Registry Viewer and FTK Imager)

Summation Certified Enduser (SCE)-Summation.

AccessData MPE+ Mobile Devices Training

Lecturer for International Legal Association (ILTA) on Social Media and electronic discovery issues. Co-Author presentation on "What Happens of FaceBook Doesn't Stay of Facebook".

Katana Lantern Examiner.

Guest speaker at Capital Law School, Electronic Discovery

Published "Electronic Discovery", in partial fulfillment of the requirements for the degree of Masters of Science in Cybersecurity

IPRO Reseller Certification – Eclipse Cloud based attorney review platform.

Completed Solo Learn SQL Fundamentals course.

Completed Solo Learn RUBY programming tutorial.

Completed Cybrary **ITIL** (Information Technology Infrastructure Library) Foundation Training.

Metasploit Pro – Rapid7 Vulnerability testing and penetration testing.

Business Intelligence Software Tableau training.

Geographical Information System (**GIS**), training in 2002 with the Columbus Dispatch, Route Smart Software for data analytics.

Department of Health and Human Services, HRQ, HCUP DATA USE AGREEMENT TRAINING

Department of the Army, United States Army Military Police School. Diploma: Protective Services Training Class 05-00

AWS Portal Partner- Experience with AWS Console, Workspaces, and Security.

Andrew Keck – Expert Witness & Cyber Security Consultant

HCUP Data Usage Agreement Training – Healthcare Cost and Utilization Project – HCUP 28L30EVW7

Electronic Discovery & Forensic Investigation Experience

The following are samples of cases that I have been named as an expert, but the case is pending, has settled outside of court or I have been a consulting expert and have not been disclosed. To protect the privacy of these cases, only generalities have been presented. I can provide further information, within the confines of any privacy issues and non-disclosure agreements, should you deem it necessary to gain further information.

FTC Matter No. 1623208, United States of America Federal Trade Commission, Washington, D.C. 20580. Forensic Expert.

Consumer Financial Protection Bureau v. Nationwide Biweekly Administration, Inc., et al., Case No. 3:15-cv-02106-RS (EDL). Expert Witness, Discovery Dispute re Defendants' Production of emails.

United States Securities and Exchange Commission, Washington, D.C. 20549. Vera Bradley – Electronic Evidence Consultant.

Community Building Systems, Inc., et al., v. Webster Bank, N.A., et al., Judge Hogan. Case No. 07CVH 06 7861. Testified via Affidavit. Forensically Collected Network Email and analyzed information produced.

Kimberly James, et al., v. Broadwin Housing Limited Partnership, et al., Judge Hogan. Case No. 08CVH 07 10582. Testified via Affidavit.

Sam Han, Ph.D., Plaintiff, v. University of Dayton, et al. The Common Pleas Court of Montgomery County, Ohio Civil Division. Provided Affidavit after forensic investigation.

Flairsoft Ltd., v. Yogesh Khandelwal, et al, Case NO: 11-CV-H-09-1107. Judge W. Duncan Whitney. In The Delaware County, Ohio Court of Common Pleas. Case Category: H. Affidavit provided. Scheduled to Testify September, 2014.

Dora Oatman, et al., v. Infocision, Inc., et al., Case NO. 12-cv-02770. In The United States District Court Northern District of Ohio Eastern Division. Judge James S. Gwin. Magistrate Judge Greg White. Coordinated Forensic data collection efforts including exchange email, VM desktop and network data.

Cranel Inc., v. ProImage Consultants Group, LLC, et al. Case NO. 2:13-cv-00766-JLG-MRA. United States District Court, Southern District of Ohio. Expert Consultant.

Andrew Keck – Expert Witness & Cyber Security Consultant

Mission Essential Personnel, LLC, v. Michael Fuqua Case NO. 12CV000288. Judge Lynch. Magistrate McCarthy. In The Court of Common Pleas Franklin County, Ohio. Expert Consultation and Forensic examination of evidence.

The Medical Center at Elizabeth Place, LLC, v. Premier Health Partners, et. al. Case NO. 3:12-cv-00026-TSB. Judge Timothy S. Black. In The United States District Court For The Southern District Of Ohio Western Division. Forensic Expert pending.

Crown Equipment v. Joe Ritter. Performed forensic collection of hard drives.

Continuing Health Care Solutions, Inc. Adv. Foundations Health Solutions, et al. Logical forensic collection and reporting of mobile devices.

Polymera (Potential non-compete violation investigation) – no case filed. Forensic investigation of Mac laptop.

Virginia Denbow v. Central Ohio Ear, Nose & Throat, Inc. (Ohio Civil Rights Commission Charge No. Col E1(39270) 03232012. Forensic investigation of multiple PC's.

Grandview Studio of Visual Arts (Ohio Attorney General investigation regarding non-profit status) – no case filed. Forensic investigation of PC and MAC computers.

NPSC Limited v. Design Collective Architecture Incorporated
Jeffrey R. Corcoran, Allen Kuehnle Stovall & Neuman LLP
Cloud based email collection.

City of Columbus v. Lyft, Inc., et al., Franklin County Municipal Court Environmental Division. Case No. 2014 EVH60145.
Cloud based collections.

PEA Lit, LLC v. Benchmark Design U.S.A., Inc., et al. Case No. 52 158 J 00613 10. Processed digital evidence, extracting metadata & text, creating load file overlays for database review.

David Fulmer v. West Licking Joint Fire District, Licking County Court of Common Pleas, Case No. 12 CV 01495
Expert Testimony.

CHARLES EDWARD BOURNE II Plaintiff, VS. BLUEMILE, INC., et al. Defendants/Third Party Plaintiffs VS. IPOUTLET, LLC c/o David Ferris, Statutory Agent The Ferris Law Group LLC P.O. Box 1237, 6797 N. High Street, Suite 214, Worthington, Ohio 43085-1237 and YOURCOLO, LLC. c/o Barry H. Wolinetz, Statutory Agent. 250 Civic Center Drive, Suite 100. Columbus Ohio 43215. IN THE COMMON PLEAS COURT OF FRANKLIN COUNTY, OHIO, CASE NO. 14 CV 005576. Also, TODD BLANK, Plaintiff, VS. BLUEMILE INC., et al., Defendants. CASE NO. 14 CV 005591. Judge Holbrook. Provided expert Testimony-affidavit.

Andrew Keck – Expert Witness & Cyber Security Consultant

GARY ONADY, Plaintiff, -vs- WRIGHT STATE PHYSICIANS, INC., Defendants. IN THE COMMON PLEAS COURT OF MONTGOMERY COUNTY, OHIO. CASE NO. 2012 CV 07251. JUDGE DENNIS J. LANGER; MAGISTRATE DAVID H. FUCHSMAN. Expert testimony and affidavit.

Ologie, LLC V. One Sixty Over Ninety, LLC, et al..
In the Court of Common Pleas Franklin County, Ohio. Judge Kim J. Brown; Magistrate Tim Harildstad. MacBook Air Forensics and expert witness consulting.

WILLIAM E. STILSON V. GLAUS, PYLE, SCHOMER, BURNS, & DEHAVEN, INC., JUDGE SEROTT. CASE NO. 16CV-00-7852. IN THE COURT OF COMMON PLEAS, FRANKLIN COUNTY, OHIO: Mobile device forensics, iCloud and iPhone.

SMITH AND CONDENI, et al., Plaintiffs, vs. JOSEPH A CONDENI, et al., Defendants. IN THE COURT OF COMMON PLEAS CUYAHOGA COUNTY, OHIO. CASE NO.: CV-17-889339. JUDGE: ASHLEY KILBANE. Expert testimony-affidavit. Cloud Email Collection.

ATLAS NOBLE, LLC, ATLAS RESOURCES, LLC, ATLAS RESOURCES SERIES 32-2012 L.P., ATLAS RESOURCES SERIES 33-2013 L.P., and ATLAS RESOURCES SERIES 34-2014 L.P., *Plaintiffs*, v. PIN OAK ENERGY PARTNERS LLC, *Defendant*. IN THE DISTRICT COURT OF HARRIS COUNTY, TEXAS 189TH JUDICIAL DISTRICT. CAUSE NO. 201949950. Expert Testimony-affidavit. Mobile Forensics & Electronic Discovery.

Midwest Motor Supply Co., Plaintiff, v. Richard H. Lamoureux, et al., Defendants. IN THE COURT OF COMMON PLEAS FRANKLIN COUNTY, OHIO. No. 17-CV-009506. Judge Christopher M. Brown. Expert Testimony-Affidavit. Forensic & Electronic Discovery.

Affiliations

Association of Litigation Support Professionals (ALSP)

Ashland University Alumni

Electronic Discovery Group

International Legal Technology Association (il+^)

Legal IT Network & Summation User Group

Utica College Alumni

Andrew Keck – Expert Witness & Cyber Security Consultant

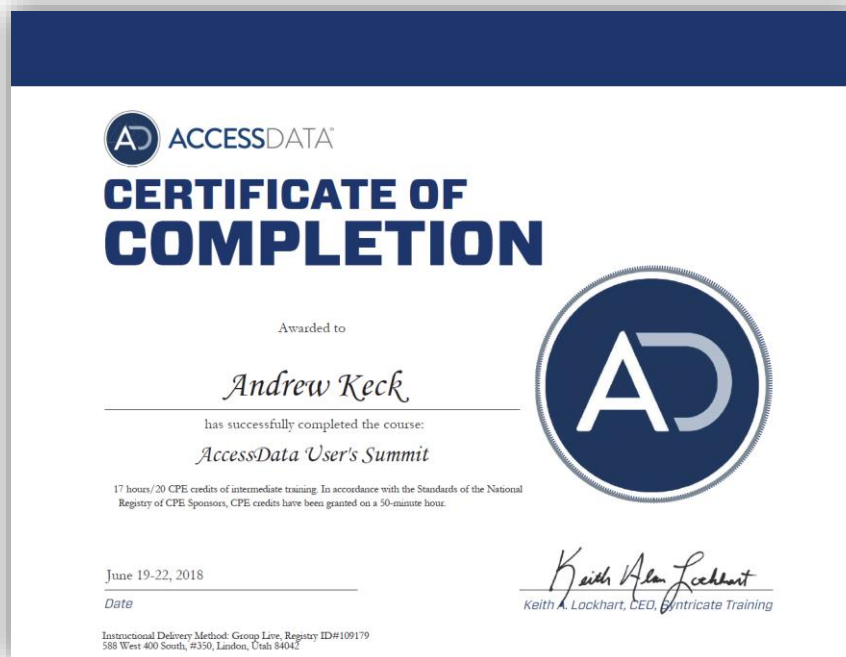


Exhibit E

Jane Ginn, MSIA, MRP

Twitter: @CTIN_Global

LinkedIn: <https://www.linkedin.com/in/janeginn>

PRINCIPAL CYBERSECURITY THREAT ANALYST

Analyst with proven knowledge of threat intelligence platforms and the tools/techniques for analyzing cyber observables and interpreting these data for conversion into actionable intelligence. Leader/manager with over 35 years of experience. Co-Secretary of the OASIS Cyber Threat Intelligence – Technical Committee (CTI TC) and Secretary of Threat Actor Context TC. Speaker at national and international conferences. Appointed advisor to the EU's ENISA, Threat Landscape Stakeholders Group. Board Member, Cyber Resilience Institute, Sponsor of the Sports Information Sharing and Analysis Organization (Sports-ISA). Adjunct faculty at Gannon University (Erie, Pennsylvania).

- | | |
|---|--|
| ✓ STIX2/TAXII2 Architecture | ✓ Cyber Threat Hunting Analysis Training |
| ✓ ISAC-ISA Set-up and Administration | ✓ Cloud Services Threat Analysis |
| ✓ Cybersecurity Intelligence Platform Testing & Admin | ✓ Risk Management |
| ✓ Regulatory Compliance Planning/Auditing | ✓ Governance and Compliance |

Career Highlights

Cyber Threat Intelligence Network, Inc.

2014-Present

President / Senior Cyber Threat Analyst

- Ran cyber threat hunting R&D Program for SASE firm with 22 subcontractors
- Adjunct Faculty for Gannon University's Computer and Information Science Department
 - Teach courses on network engineering and cybersecurity management
- Developer of curriculum for c-Watch & CrowdWatch programs for Sports-ISA
- Website designer for multiple e-commerce enabled sites serving cross-sector customers
- Analyst for business viability of non-fungible tokens (NFTs) for digital assets
- Administrator of Threat Intelligence Platforms (TIPs) for multiple ISACs/ISAOs
- Member of planning team for national cybersecurity critical infrastructure exercise
- Developer of curriculum for cybersecurity training programs and internship programs
- Provider of consulting services for MITRE, US DHS & Cyber Resilience Institute
- Presenter at multiple ENISA meetings on cyber threat intelligence (Brussels, Rome, Bern)
- Guest lecturer at Duke U., Northern Arizona U., Great Lakes U. (Chennai, India) & others

University of Phoenix

2003 – 2012

Faculty, Certified Advanced Facilitator

- Taught courses in international business & information systems and technology
- Taught in all modalities (on-ground, FlexNet, and online)

CG Maersk, USA

2002 – 2003

General Manager, West Coast Operations

- Performed business development for India-based software engineering teams
- Formed strategic alliances for global delivery of IT & software engineering services
- Negotiated terms and conditions for global IT delivery infrastructure

Max Foundation

2000 – 2002

Director of Operations

- Set-up/administered HR and IT units for global delivery of cancer care program
- Oversaw software engineering design of global platform for working with oncologists

US/Mexico Chamber of Commerce, NW Chapter

1998 – 1999

Executive Director

- Set-up/administered Northwest Chapter in Seattle, WA
- Liaison officer during World Trade Organization meetings in Seattle
- Advance planning and trade mission support for Governor's Mexico trade mission

Ginn & Associates

1993 – 1998

Consultant

- Served on Federal Advisory Board (ETTAC) on international trade
 - Appointed by 5 consecutive Secretaries of the US Department of Commerce
- Provided international trade analysis and facilitation for multiple private clients
- Conducted in-country business competitive research and analysis for US Embassy - Argentina
- Supported due diligence activities for private acquisitions
- Hosted multiple trade delegations from Asian and Latin American countries

Hart Crowser

1990 – 1993

Project Manager

- Provided air quality auditing support at US DOE's Hanford site
- Managed regulatory compliance task for high level tanks pilot project at Hanford
- Managed field investigation teams for assessing environmental risks at properties for a major Pacific Northwest regional bank

Ebasco Environmental

1988 – 1990

Regulatory Analyst

- Worked on multiple hazardous, radioactive and mixed waste task under contract at DOE's Hanford site
- Provided Environmental Impact Statement support for NASA Solid Rocket Booster program

NUS

1984 – 1988

Regulatory Analyst

- Developed database for groundwater monitoring wells at DOE's Savannah River Plant
- Provided regulatory analysis (NRC, EPA) on high-level nuclear repository project
- Managed regulatory development task for EPA's hazardous waste management program
- Conducted audits of state regulatory programs for as member of EPA audit team

Education

- Master of Science in Information Assurance, Norwich, Northfield, VT – 2014 (4.0 GPA)
 - Applied Information Technology (AIT) Certificate, ITI, Bellevue, WA – 2001
 - Master of Environmental Science and Regional Planning (MRP), Washington State, Pullman, WA – 1988
 - Bachelor of Arts (BA), Geography, U. of Oklahoma, Norman, OK - 1981
-

Multiple publications. Copies provided upon request. | References available upon request.

Clearances: Secret | Public Trust | Federal Advisory Board